Posted to DOJ OIG FOIA Reading Room After Earlier FOIA Release

DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

REPORT OF INVESTIGATION

SUBJECT	CASE NUMBER
(b)(6); (b)(7)(C) (***-**-(b)(6); (b)(7)(Special Agent in Charge (former) (b)(6); (b)(7)(C)	2024-000308

OFFICE CONDUCTING INVESTIGATION	DOJ COMPONENT
(b)(6); (b)(7)(C)	Drug Enforcement Administration

DISTRIBUTION	STATUS
☒ Region (b)(6); (b)(7)(	☐ OPEN ☐ OPEN PENDING PROSECUTION ☒ CLOSED
☒ AIGINV	PREVIOUS REPORT SUBMITTED: ☐ YES ☒ NO
☒ Component DEA	Date of Previous Report:
☐ USA	
☐ Other	

SYNOPSIS

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the Drug Enforcement Administration (DEA) Office of Professional Responsibility (OPR) alleging that on (b)(6); (b)(7)(C) DEA (b)(6); (b)(7)(C) Special Agent in Charge (SAC) (b)(6); (b)(7)(C) remotely monitored an unauthorized camera located in the SAC's office. The information indicated that (b)(6); (b)(7)(C) may have used the camera to monitor the activities of individuals using the SAC's office without the knowledge of those individuals.

The OIG investigation substantiated the allegation that (b)(6); remotely monitored an unauthorized camera located in the SAC's office, in violation of DEA policy.

A Blink Mini camera was retrieved from the SAC's office by (b)(6); (b)(7)(C) management on (b)(6); (b)(7)(C) Amazon records and Wi-Fi network logs revealed that on (b)(6); (b)(7)(C) the Blink Mini camera was connected to an unsecure public Wi-Fi network located at the DEA (b)(6); office and remained connected until (b)(6); (b)(7)(C) Amazon records confirmed the Blink Mini camera was owned by (b)(6); (b)(7)(C)

Four witnesses told the OIG that they observed the camera in plain view in the SAC's office.

DATE March 20, 2025	SIGNATURE (b)(6); (b)(7)(C) Digitally signed by (b)(6); (b)(6); Date: 2025.03.20 15:00:35 -06'00'
(b)(6); (b)(7)(C) PREPARED BY SPECIAL AGENT	
DATE March 20, 2025	SIGNATURE Keith A. Bonanno Digitally signed by KEITH BONANNO Date: 2025.03.20 16:08:24 -06'00'
Keith Bonanno APPROVED BY SPECIAL AGENT IN CHARGE	

Portions of the Report of Investigation may not be exempt under the Freedom of Information Act (5 U.S.C. § 552) and the Privacy Act (5 U.S.C. § 552a).

Posted to DOJ OIG
FOIA Reading Room After
Earlier FOIA Release

The OIG also reviewed text message communications between (b)(6); and DEA (b)(6); (b)(7)(C) about activity in the SAC office, which revealed that (b)(6); remotely monitored the camera when he was not in the office.

In a voluntary interview, (b)(6); admitted that he installed a personally-owned Blink Mini camera in his office, sometime in (b)(6); (b)(7)(C) or early (b)(6); and said he had done so to safeguard his belongings from "floods" when he was not in the office. (b)(6); said he accessed live view via the Blink application (app) on his DEA-issued iPhone and iPad to see and hear what the camera was capturing in the moment, but did not knowingly create or save recordings. (b)(6); DEA-issued iPhone and iPad had been factory reset prior to initiation of the OIG investigation.

(Destruction of evidence in a federal investigation)

The U.S. Attorney's Office (b)(6); (b)(7)(C) declined prosecution of (b)(6); The U.S. Attorney's Office (b)(6); (b)(7)(C) was recused from this matter.

(b)(6); was removed from his position by the DEA effective (b)(6); (b)(7)(C) removal was for misconduct unrelated to the OIG investigation.

The OIG has completed its investigation and all criminal and administrative actions are complete. The OIG is providing this report to the DEA for its information.

Unless otherwise noted, the OIG applies the preponderance of the evidence standard in determining whether DOJ personnel have committed misconduct. The Merit Systems Protection Board applies this same standard when reviewing a federal agency's decision to take adverse action against an employee based on such misconduct. See 5 U.S.C. § 7701(c)(1)(B); 5 C.F.R. § 1201.56(b)(1)(ii).

Posted to DOJ OIG
FOIA Reading Room After
Earlier FOIA Release

DETAILS OF INVESTIGATION

Predication

The Department of Justice (DOJ) Office of the Inspector General (OIG) initiated this investigation upon the receipt of information from the Drug Enforcement Administration (DEA) Office of Professional Responsibility (OPR) alleging that on (b)(6); (b)(7)(C) DEA (b)(6); (b)(7)(C) Special Agent in Charge (SAC) (b)(6); (b)(7)(C) remotely monitored an unauthorized camera located in the SAC's office. The information indicated that (b)(6); may have used the camera to monitor the activities of individuals using the SAC's office without the knowledge of those individuals.

Investigative Process

The OIG's investigative efforts consisted of the following:

Interviews of the following DEA personnel:

(b)(6); (b)(7)(C) former Special Agent in Charge

(b)(6); (b)(7)(C)

Review of the following:

(b)(6); (b)(7)(C) DEA email communications for the period of (b)(6); (b)(7)(C) to (b)(6); (b)(7)(C)

- Amazon records for (b)(6); personally-owned Blink Mini camera
- City and County of (b)(6); Wi-Fi network logs

(b)(6); (b)(7)(C)

- (b)(6); (b)(7)(C) building access logs
- (b)(6); eOPF file

Background

(b)(6); transferred to the (b)(6); office as the Special Agent in Charge in (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

On (b)(6); (b)(7)(C) was removed from his position by the DEA for misconduct unrelated to OIG's investigation.

DEA turned over the camera retrieved from the SAC office to the DOJ OIG on (b)(6); (b)(7)(C) The camera was identified as a black Blink Mini camera with a unique serial number and Media Access Control (MAC) address. Blink is an Amazon-owned company. A search of Amazon's public webpage identified an Amazon Product Detail Page

Posted to DOJ OIG FOIA Reading Room After Earlier FOIA Release

specific to the Blink Mini camera which described the camera as a compact indoor, plug-in smart security camera with motion detection and two-way audio. The description further specified a user can see, hear, and speak to people from a smartphone with the Blink Mini's live view and two-way audio features.

(b)(6); (b)(7)(C) Installed and Remotely Monitored an Unauthorized Personally-Owned Camera in the (b)(6); (b)(7)(C) SAC's Office

The information provided to the OIG alleged that on (b)(6); (b)(7)(C) remotely monitored an unauthorized camera located in the (b)(6); (b)(7)(C) SAC's office. The information indicated that (b)(6); (b)(7)(C) may have used the camera to monitor the activities of individuals using the SAC's office without the knowledge of those individuals.

DEA policy provides the following:

Offense Code 2735.20(J) Unauthorized Recording of Employee Conversations: DEA employees are prohibited from recording conversations of another individual without the mutual consent of all parties, except in the conduct of bona fide official investigations under the auspices of the OPR or other appropriate organization.

Offense Code 2735.20(B)(5) DEA Records and Official Information: Employees will comply with all applicable regulations, guidance, and policy regarding the safeguarding, review, and removal of documents by DEA personnel, the maintenance of personal papers by DEA personnel, and the security and integrity of official records. No employee shall acquire, distribute, or maintain (either intentionally or in a negligent manner) administratively controlled, privileged, or classified information from another agency, person, or entity under false pretenses.

Offense Code 2735.18(B)(1) Use of Government Property: All employees are required to properly use and protect all equipment and supplies issued to or used by them. DEA personnel are to safeguard property in their possession, control, or work-area. Government property will only be used for officially approved purposes and will not be used for personal use or benefit, except for such de minimis use which involves negligible or no expense to the Government and does not interfere with or otherwise impede official business. This limited authority, i.e., to make de minimis use of government property or materials, does not permit an employee to access administratively controlled information for his/her personal use or to access informational databases.

(b)(6); (b)(7)(C) told the OIG that on (b)(6); (b)(7)(C) at 2:29 PM, she received a text message from (b)(6); (b)(7)(C) which stated, "Wow. Now (b)(6); (b)(7)(C) is using my office. What's next [face with rolling eyes emoji]." At the time of (b)(6); (b)(7)(C) text message, (b)(6); (b)(7)(C) responded, "How did you know?" and (b)(6); (b)(7)(C) replied, "I know." (b)(6); (b)(7)(C) continued texting (b)(6); (b)(7)(C) "It doesn't matter, I was just curious. Of all people it would be him. It's not really 'my' office anyways -- but gwiz please keep my stuff orderly and clean." "I prefer that nobody use my office unless all my stuff is moved out -- especially when people are in there with the door closed and I have personal items/documents in drawers and cabinets there." The text messages were received by (b)(6); (b)(7)(C) shortly after (b)(6); (b)(7)(C) went into the SAC's office to work and meet with (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) Large pieces of paper were taped to the windows in the SAC's office and used for meeting notes. The next morning, (b)(6); (b)(7)(C) removed the meeting notes from the windows and reported the text messages she received from (b)(6); (b)(7)(C) to (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) previously advised (b)(6); (b)(7)(C) prior to (b)(6); (b)(7)(C) that there may be a camera in (b)(6); (b)(7)(C) office and recommended she not make personal calls in the SAC's office. (b)(6); (b)(7)(C) told the OIG that prior to (b)(6); (b)(7)(C) she observed a black camera in (b)(6); (b)(7)(C) office but could not recall the first time she saw the camera. The camera was in plain view on top of the cabinet/desk against the wall. Even with previous knowledge of the camera's existence, (b)(6); (b)(7)(C) utilized (b)(6); (b)(7)(C) office for privacy to make personal phone calls when (b)(6); (b)(7)(C) was out of the office. (b)(6); (b)(7)(C) continued making personal phone calls in (b)(6); (b)(7)(C) office after (b)(6); (b)(7)(C)

Posted to DOJ OIG FOIA Reading Room After Earlier FOIA Release

told the OIG that he was instructed by OPR to retrieve a camera from the SAC office on Two hours after retrieved the camera, appeared in office without any prior notification. advised that on he received an email that he had been terminated by the DEA and he was there to clean out his office. Within minutes of going into the SAC office, reapproached and questioned him about the whereabouts of his camera. told he was directed by OPR to take the camera. questioned if there was anything wrong with the camera and asked if he could get it back. told he was waiting on OPR to advise him on what to do next. told he had the camera since "day one" and used it to look at the weather from his house. After packed up his office, and drove to home to retrieve assigned government property. While at home, drew attention to a camera in the house, and commented that he used the camera to watch the weather and explained the camera does not stream or record, but he had to be logged in to see the weather. also asked if the camera (located in his DEA office) was going to be an issue, to which responded he did not know what to say said office was utilized by other DEA employees on multiple occasions between and Employees used office for official business and for privacy to make personal phone calls. further stated it was reasonable to believe that Law Enforcement Sensitive (LES) information was discussed in office.

told the OIG that he first noticed the camera in office at some point after arrived at the office in and a couple times since, when he was in office. said the camera sat on top of the taller cabinet behind desk and it was placed in open view and positioned toward the big windows in the office. did not know if the camera was recording. estimated a hundred people went in and out of office since arrived at the and no one previously mentioned the camera to stated it is reasonable to believe that LES information, Personally Identifiable Information (PII), and sensitive personnel matters were discussed in office while was not physically present in the office. At times, participated in the discussion of personnel matters with and employees in office.

told the OIG that she first observed a camera in office after made a comment and joked about a camera in the SAC's office, although she was unable to recall when she first saw the camera. Other than did not hear anyone else comment that they saw a camera in office. described the camera as being in plain view, and said it was not hidden or camouflaged. said she and utilized office for privacy to make personal phone calls. job duties included managing access to office, and she had the code to access the office. also had codes to access the office.

An OIG review of the building access logs confirmed that only accessed the office on one occasion between and which is consistent with the witness statements. This one occasion was on

The OIG reviewed records provided by the City and County of that revealed an unsecured public Wi-Fi network named "GuestWiFi" was setup by the City and County of at the office. According to Internet Protocol (IP) connection logs provided by the City and County of the Blink Mini camera was attached to the city Wi-Fi network from to and continually established connections out to Amazon.

The OIG's review of Amazon records revealed the Blink Mini camera was first connected to a network on On this date, the network name changed from "Home" to "DEA" and remained "DEA" until it was

Posted to DOJ OIG
FOIA Reading Room After
Earlier FOIA Release

deleted on (b)(6); (b)(7)(C) The account was associated to a user with the email address "(b)(6); (b)(7)(C)" The "(b)(6);" appears to represent the first and last initials of (b)(6); name.

A review of the command history records obtained from Amazon and associated to the camera revealed approximately 1,133 instances where a user initiated the "live view" command from an iPad or iPhone to access real-time video and audio from the camera. On (b)(6); (b)(7)(C) the date (b)(6); texted (b)(6); at 2:29 PM about activity in the SAC's office, live view was accessed four times at 2:21:31 PM, 02:25:18 PM, 02:38:20 PM, and 02:45:37 PM. It appears four media clips corresponding to the live view sessions were saved, including 43 seconds saved at 2:22:16 PM, 86 seconds saved at 2:26:46 PM, 31 seconds saved at 2:38:53 PM, and 27 seconds saved at 2:46:06 PM (b)(6); According to Amazon, recordings are hard deleted once the created at date is older than the auto-purge days, which was set to 3 days. Approximately 1,027 media records associated to the Blink Mini camera were deleted from (b)(6); (b)(7)(C) to (b)(6); (b)(7)(C) All but one record was deleted by a user. The remaining one record was deleted by the cleanup process due to auto-purge or limit exceeded. The length of the deleted media varied from 0 to 90 seconds. Factually provable lie to investigators - Can 'we' get away with this? No.

A review of (b)(6); DEA email account revealed emails from (b)(6); (b)(7)(C) to (b)(6); (b)(7)(C) the email account associated to (b)(6); Blink Amazon account. The review did not identify that (b)(6); sent any sensitive, non-public information from his DEA email account to his personal email account.

A review of (b)(6); eOPF file revealed that, since (b)(6); in conjunction with (b)(6); annual performance appraisal record, (b)(6); acknowledged he read and understood the DEA's Standards of Conduct, to include question #9, which reads: "Unauthorized Recording of Employee Conversations. Are you aware that you, as a DEA employee, may not record conversations of other employees without the consent of all parties, except in the conduct of officially authorized investigations?"

In a voluntary interview, (b)(6); stated he installed a personally-owned Blink Mini camera in his office around the first time it "flooded", sometime in (b)(6); or early (b)(6); (b)(7)(C) explained his office flooded about three or four times when rain leaked into the building through degrading rubber gaskets around the windows and exterior door. (b)(6); said he had thousands of dollars' worth of police collectibles and electronics in his office that he worried would get damaged in a subsequent flood, and therefore installed the camera to safeguard his personal belongings when he was not in the office. (b)(6); stated he placed the camera on top of his desk where it was not hidden and angled the camera out the front window so he could see the weather, as rain or snow could potentially cause his office to flood.

(b)(6); stated that he connected the camera to the (b)(6); (b)(7)(C) (b)(6); Wi-Fi network, which was commanded by the (b)(6); Police Department and located at the DEA (b)(6); office. (b)(6); said he set the camera up as a standalone camera, without a sync module or Secure Digital (SD) card. An SD card is used to store video clips directly from the camera system and a sync module allows cameras to save clips to cloud storage for a maximum of 60 days before auto-deleting. The camera was not part of a Blink subscription plan, although (b)(6); had a Blink account and accessed the Blink app to view the camera from his DEA-issued iPhone and iPad. (b)(6); confirmed his personal email address, (b)(6); (b)(7)(C) was associated to the Blink account.

Within the Blink account, (b)(6); labeled his cameras, which included cameras located at his home. (b)(6); said he labeled the camera at the DEA "office or something like that." (b)(6); stated no one else had remote access to the Blink camera at the DEA (b)(6); office. (b)(6); stated he accessed live view to see and hear what the camera was capturing in the moment but was adamant he did not knowingly create or save any recordings.

Posted to DOJ OIG FOIA Reading Room After Earlier FOIA Release

(b)(6); was asked what prompted the text message he sent to (b)(6); (b)(7)(C) when (b)(6); was in the SAC office. (b)(6); did not recall the exact wording of the text but explained the circumstances surrounding the message. Initially, (b)(6); stated, "I can't remember how – I either knew or was made aware or the weather, I honestly don't remember. I just knew that there was something, there was a problem – there may have been potential flooding or something. I can't remember if somebody told me or if I had been monitoring the weather and was concerned. I don't know. No one ever told me that the office had flooded. I turned the camera on to check and there were fans going. The internet connection to that camera was very poor." When asked again what prompted him to send the text message to (b)(6); (b)(7)(C) stated, "I remember that that week (b)(6); (b)(7)(C) (b)(6);), there was a problem. I don't remember how I was made aware of it, whether it was a hunch on my part or what, but I turned the camera on to check, because like I said, everyone stopped calling me. And it was a surprise to me that there was [moisture] mitigation stuff going on in there, and that's when I saw an individual on the righthand side of the camera, sitting, again, totally unexpected to me." (b)(6); said that seeing an individual in his office "greatly bothered" him because of the "circumstances that surrounded that." (b)(6); stated that when he was out of the office, his office was always locked with the added protection of a cipher code on the door. (b)(6); did not have knowledge of staff using his office.

(b)(6); told the OIG that the SAC office experienced ongoing flooding issues and provided limited building maintenance logs that revealed water damage following a rainstorm in (b)(6); (b)(7)(C) The logs showed that on (b)(6); (b)(7)(C) a rainstorm was reported to have caused leaking around windows and doors and water damage on ceiling tiles within the (b)(6); office. Email communication from DEA staff to building maintenance personnel confirmed the SAC office was affected by the rainstorm. On (b)(6); (b)(7)(C) a commercial restoration company was onsite for abatement and left fans running to dry out the affected area until (b)(6); (b)(7)(C) On (b)(6); (b)(7)(C) (b)(6); the logs reported that "window molding by the SAC office is coming apart," and on (b)(6); (b)(7)(C) "ceiling tiles damaged from flood" were replaced.

(b)(6); was unable to provide maintenance logs regarding flooding in (b)(6); (b)(7)(C) however, OIG Agents observed two fans and an extension cord on the floor of the SAC office on (b)(6); (b)(7)(C) which were likely there to mitigate moisture.

The OIG issued a subpoena to (b)(6); to produce any recordings from the Blink camera that were in his possession, custody, and/or control, and (b)(6); responded through his attorney that he did not have any recordings that were responsive to the subpoena.

The U.S. Attorney's Office (b)(6); (b)(7)(C) declined prosecution of (b)(6); (b)(7)(C) The U.S. Attorney's Office (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) was recused from this matter.

(b)(6); was removed from his position at the DEA effective (b)(6); (b)(7)(C) removal was for misconduct unrelated to the OIG investigation.

OIG's Conclusion

The OIG investigation concluded that (b)(6); installed and remotely monitored an unauthorized personally-owned camera located at the DEA office as alleged, in violation of DEA policy. The OIG investigation revealed that between (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C) personally-owned Blink Mini camera was installed at the DEA (b)(6); (b)(7)(C) SAC office and connected to an unsecured public Wi-Fi network owned and operated by the City and County of (b)(6); During this time, (b)(6); remotely monitored activity in the SAC office and accessed real-time video and audio from the camera without the consent of the persons whose conversations were monitored or recorded.

Posted to DOJ OIG
FOIA Reading Room After
Earlier FOIA Release

(b)(6); created federal records by electronically recording official government business conducted in the SAC office. The records were electronically transmitted over an unsecure, non-DOJ Wi-Fi network to Amazon's servers and were maintained in (b)(6); Amazon Blink account until deleted. Although the content of the recordings is unknown, it can be assumed that LES information, PII, and sensitive personnel matters were transmitted and recorded without safeguarding the security and integrity of official records. (b)(6); stated he did not knowingly create or save recordings.

(b)(6); office was located behind an access-controlled door within a secure government building. Few people had direct access to (b)(6); work-area. (b)(6); exhibited disregard for the established physical security measures within the government facility when he installed a personally-owned camera in the SAC office and transmitted the audio and video activity from the law enforcement sensitive space for his personal use.

Lastly, (b)(6); circumvented the security controls on Department systems by utilizing a non-DOJ Wi-Fi network installed at the (b)(6); office for the purpose of official business in order to connect his personally-owned camera.